

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of:

Dropbox ID User # 1027006608, user name of "Laural Raines" and email address of lauralraines@gmail.com and all its associated services including deleted files and e-mails; IP addresses and associated dates/times used to access the e-mail account; activity history; that is/are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., 185 Berry Street, San Francisco, CA 94107.

Case No. 19-MJ-1372

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

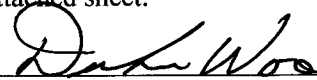
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Section 2252A.

The application is based on these facts: See attached affidavit.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



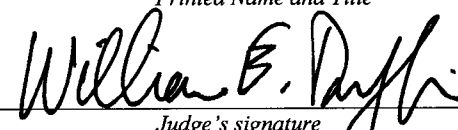
Applicant's signature

FBI Task Force Officer Dickson

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 12/11/19



Judge's signature

City and State: Milwaukee, Wisconsin

Hon. William E. Duffin, U.S. Magistrate Judge

Printed Name and Title

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Dickson Woo, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., an online, electronic file storage provider headquartered at 185 Berry Street, 4<sup>th</sup> Floor, San Francisco, California 94107. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Task Force officer with the Federal Bureau of Investigation (FBI), and have been since January, 2015 I am assigned to the FBI's Child Exploitation Task Force, Milwaukee Division. My duties include investigating violations of federal criminal law, including violations of Title 18, United States Code, Section 2252, which criminalizes accessing with intent to view, possession, receipt, and distribution of child pornography. I have gained experience in conducting these investigations through training and through everyday work, to include executing search warrants and conducting interviews of individuals participating in the trading and manufacturing of child pornography. I have also received training relating to the investigation of Internet Crimes against Children (ICAC) which includes training in the investigation and enforcement of state and federal child pornography laws in which computers

and other digital media are used as a means for receiving, transmitting, and storing child pornography.

3. As a Federal Task Force officer, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States. In particular I investigate violations of Title 18, United States Code, Sections 2251 and 2252A which criminalize, among other things, the production, advertisement, possession, receipt, and transportation of child pornography.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A have been committed by Dennis Czysz Jr. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

#### **DEFINITIONS**

6. The following definitions apply to the Affidavit and Attachments A and B to this Affidavit:

a. "Cellular telephone" or "cell phone" means a hand held wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone

usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

b. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

d. "Computer Server" or "Server," is a computer that is attached to a

dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

e. "Computer hardware" means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

j. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the



Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. "Internet Service Providers" (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

l. "An Internet Protocol address" (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most

Internet service providers control a range of IP addresses. Some computers have static, that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

m. "Hash Value" refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a "digital fingerprint" for data. If the data is changed, even very slightly (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means that the digital photo is an exact copy of the known file.

n. "Media Access Control" (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

o. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

p. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in



handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

q. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

r. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

#### **PROBABLE CAUSE**

6. The National Center for Missing and Exploited Children (NCMEC) provided NCMEC Cyber tip # 41119460 involving an individual who resides in the Milwaukee area and has a history of possessing child pornography. The complaint was filed by Dropbox to NCMEC on October 3, 2018. The complaint stated there were approximately 141 videos of suspected

child pornography uploaded to the Dropbox account created by the email address of lauralraines@gmail.com, the screen name of Laural Raines, and the ESP user ID of 1027006608.

7. NCMEC served an administrative subpoena to Charter Communications for the IP address associated (2605:a000:b141:3400:a176:3fac:272a:f87a) with the Laural Raines Dropbox account for September 30, 2018. The IP address resolved to Dennis Czysz, 3657 E. Layton Avenue, Apt. 7, Cudahy, Wisconsin.

8. NCMEC served an administrative subpoena to Google, Inc regarding the email address of lauralraines@gmail.com that was used to register for the Dropbox account. Google responded with that the email was listed to a Laural Raines, created on 04/13/2018 02:32:54-UTC, (414) 412-2487- T-Mobile, Google account number 417602629805.

9. NCMEC served an administrative subpoena to T-Mobile regarding the phone number of (414) 412-2487. T-Mobile responded with the subscriber information for the telephone number as listing to Dennis Czysz of 822 N. 24<sup>th</sup> Street, Milwaukee, WI 53233, Start time: Dec 15, 2017 08:00:00 (UTC), End time: Jan 01, 0001 08:00:00 (UTC).

10. A check on search databases such as CLEAR and Accurint showed Dennis Czysz resided at 3657 E. Layton Ave Apt #7, Cudahy, WI in 2018. Through a check with the Wisconsin Department of Corrections (WI DOC) it showed Czysz as a registered sex offender in the State of Wisconsin and they had Dennis Czysz currently residing at 3803 W. National Ave Apt# 3, West Milwaukee, WI 53215. Dennis Czysz's Wisconsin Driver License also listed his address at 3803 W. National Ave Apt # 3, West Milwaukee, WI. In 2000, he was convicted of exposing a child to harmful materials and in 2005 he was convicted of possession of child pornography. WI DOC also had Czysz's contact telephone number as (414) 412-2487.

11. On June 27, 2019 a Federal Search Warrant was executed at Dennis Czysz's address of 3803 W. National Ave, Apt #3, Milwaukee, WI. Czysz and two roommates were present at the residence. Electronic devices and mediums such as laptops, cell phones and CD/DVD's were seized from the residence.

12. FBI CART (Computer Analysis Response Team) performed a forensic exam of the items, specifically the ZTE Z982 cell phone (414) 412-2487 that was found on Czysz while at the residence. A review of the forensic image of the cell phone revealed approximately 727 images that appear to be child pornography.

13. "Dropbox" refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an "offsite" storage medium for data viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

14. Dropbox provides a variety of online services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name [www.dropbox.com](http://www.dropbox.com). Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber's full name, physical address,

telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

15. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

16. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices accessed the account.

17. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications,

including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

18. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc. to disclose to the government copies of the records and other information, including the content of communications, particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

### **CONCLUSION**

19. Based on the forgoing, I request that the Court issue the proposed search warrant because there is probable cause to believe that evidence of a criminal offense, namely, a violation of 18 U.S.C. § 2252A, is located within Dropbox account(s) associated with Dropbox link files, which are more fully described in Attachment A, which is incorporated herein by reference.

20. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that — has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

21. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

## **ATTACHMENT A**

### **Property to Be Searched**

The property to be searched is the entire digital contents of the Dropbox account(s) associated with the following Dropbox subscriber name:

1. Dropbox ID User # 1027006608, user name of "Laural Raines" and email address of lauralraines@gmail.com and all its associated services including deleted files and e-mails; IP addresses and associated dates/times used to access the e-mail account; activity history; that is/are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107.



## **ATTACHMENT B**

### **Particular Items to be Seized**

#### **I. Information to be disclosed by Dropbox, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the Dropbox accounts described above, including activity history, log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting: and emails “invites” sent or received via Dropbox, and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Dropbox and any person regarding the account or identifier, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A involving the account(s) associated with the Dropbox link files referenced in Attachment A pertaining to the possession and distribution of child pornography images and/or videos.

## **III. Method of delivery**

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to TFO Dickson Woo at: Federal Bureau of Investigation, 3600 South Lake Drive, St. Francis, Wisconsin 53235.